PATENT ABSTRACTS OF JAPAN

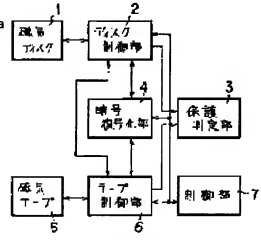
(11)Publication number : 05-233459
(43)Date of publication of application : 10.09.1993

(51)Int.Cl. G06F 12/14

(21)Application number : 04-034936 (71)Applicant : TOSHIBA CORP
(22)Date of filing : 21.02.1992 (72)Inventor : TOMOTA ICHIRO

(54) DATA BACKUP DEVICE

(57)Abstract:
PURPOSE: To encipher and back up data which should be secret.
CONSTITUTION: Data used by an information processing system for a specific process are stored on a magnetic disk 1 and a protection deciding means 3 decides whether or not all access principal bodies have the right for read access to the data read out of the magnetic disk 1 according to access right information added to the data. When it is decided that at least one of the access principal bodies does not have the right for read access are enciphered by an enciphering part 4 and recorded on a magnetic tape 5, and when it is decided that all of the access principal bodies have the right for read access, the data are recorded on the magnetic tape 5 as they are.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－233459

(43)公開日　平成5年(1993)9月10日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/14	３２０　Ｂ	9293－5Ｂ		

審査請求　未請求　請求項の数２(全　7　頁)

(21)出願番号　特願平4－34936

(22)出願日　平成4年(1992)2月21日

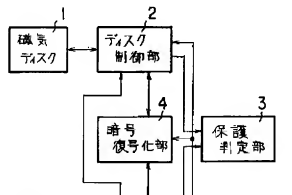
(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　友田　一郎
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝総合研究所内

(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　データバックアップ装置

(57)【要約】
【目的】本発明は、守秘の必要のあるデータについて暗号化してバックアップするようにしている。
【構成】情報処理システムでの所定の処理に用いられるデータを磁気ディスク１に記憶していて、この磁気ディスク１より読み出されたデータに対しあらかじめ付与されたアクセス権情報に基づいて全てのアクセス主体が前記データに対して読み出しアクセス権を持つか否かを保護判定部３で判定し、ここで少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについては暗号化部４で暗号化して磁気テープ５に記録し、一方、全てのアクセス主体に読み出しアクセス権を持っていると判定されたデータについては、このデータをそのまま磁気テープ５に記録するようにしている。



1

【特許請求の範囲】

【請求項1】　アクセス保護機能を備えた情報処理システムに用いられるデータバックアップ装置において、

前記情報処理システムでの所定の処理に用いられるデータを記憶する第1の記憶媒体と、

この第1の記憶媒体より読み出されたデータについてあらかじめ付与されたアクセス権情報に基づいてアクセス主体が前記データに対して読み出しアクセス権を持つか否かを判定する判定手段と、

この判定手段によりなくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについて暗号化を実行する暗号化手段と、

前記判定手段より全てのアクセス主体が読み出しアクセス権を持っていると判定されたデータについては該データをそのまま記録し前記少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについては前記暗号化手段で暗号化されたデータを記録する第2の記憶媒体を具備したことを特徴とするデータバックアップ装置。

【請求項2】　第2の記憶媒体は記録されるデータとともに該データにあらかじめ付与されたアクセス権情報を記録し、前記第2の記憶媒体より読み出されたデータに対し該データに付与されたアクセス権情報に基づいてアクセス主体が前記データに対して読み出しアクセス権を持つか否かを判定手段で判定し、該判定手段により少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについて復号化手段により復号化を実行し、前記判定手段より全てのアクセス主体が読み出しアクセス権を持っていると判定されたデータについては該データを、あるいは前記少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについては前記復号化手段で復号化されたデータをそれぞれ第1の記憶媒体に書込むことを特徴とする請求項1記載のデータバックアップ装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はアクセス保護機能を備えた情報処理システムにに用いられるデータバックアップ装置に関するものである。

【0002】

【従来の技術】最近、各種の情報処理システムが用いられているが、このようなシステムでは、故障や操作ミスが原因でデータが破壊されることが多々ある。

【0003】そこで、従来では、このような事態を想定して、システムで処理されるデータを複写して保存しておき、実際にデータが破壊された場合に、保存しておいたデータに基づいて元のデータを復元する、いわゆるバックアップを行うデータバックアップ装置が用いられている。

【0004】一方、情報処理システムでは、一般にセキュリティやプライバシを保護する目的で、許さべからざるアクセスからデータを保護するものとして、アクセス保護機能が設けられている。

2

【0005】この場合のアクセス保護機能は、アクセス権情報を設定するための手段とアクセス制御を行なう手段によって構成されている。ここで、アクセス権情報とは、システム内で処理するどのデータに対してどのアクセス主体がいかなるアクセスを行なう権利を持っているかについての情報で、アクセス主体とはアクセスを行なうもののことをいい、何を単位として個々のアクセス主体と考えるかはシステムにより異なり、例えばシステムに登録されている個々の利用者を個々のアクセス主体と考え、システム内で処理する個々のデータに対して個々の利用者がいかなるアクセスを行なう権利を持っているかという形でアクセス権情報を設定しアクセス保護を行なう場合が見受けられる。また、この他にも、システム中にある個々のコマンドを個々のアクセス主体と考えてアクセス保護を行なうものや、システムを構成する個々の処理装置を個々のアクセス主体と考えてハードウエア的にアクセス保護機能を実現するものも見受けられる。またアクセス制御手段は、アクセス主体によってデータに対しアクセスが行なわれようとした時に、前記アクセス権情報に基づいてそれが許可されるべきものか否かを判断し、許可されるべきでないアクセスを阻止することである。

【0006】

【発明が解決しようとする課題】ところが、このようなアクセス保護機能を備えた情報処理システムにおいてデータのバックアップを行なう場合、以下のような問題点が発生していた。

【0007】まず、情報処理システムにおいて処理過程にあるデータについては十分なアクセス保護をなし得ても、それをバックアップによって複写保存したものについては十分なアクセス保護を行なうのが困難なことが多く存在することである。例えば、磁気ディスク上のファイルシステムを磁気テープによりバックアップするような場合、一般にファイルシステムは磁気ディスク上のファイルに対してはアクセス保護を行うことができるが、磁気テープ上のファイルに対してまでアクセス保護を行うことができないことがある。

【0008】このような場合、磁気ディスク上にあった時にはセキュリティ保護やプライバシ保護のために読み出す権利を持つ利用者を制限したファイルであっても、それをバックアップによって記録したものについては、本来読み出す権利のない利用者にも読み出し可能な状態になってしまうことが生じる。加えて、一般にバックアップを記録するための媒体は、例えば磁気テープなどのような取替可能な媒体が使われることが多く、しかもこれら媒体は持ち運びが容易であるために、盗まれる可能性もあった。

【０００９】本発明は、上記事情に鑑みてなされたもので、バックアップによって保存されるデータに対してセキュリティ保護とプライバシ保護を安定して確保することができるデータバックアップ装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明は、アクセス保護機能を備えた情報処理システムに用いられるデータバックアップ装置において、情報処理システムでの所定の処理に用いられるデータを記憶する第１の記憶媒体、この第１の記憶媒体より読み出されたデータについてあらかじめ付与されたアクセス権情報に基づいてアクセス主体が前記データに対して読み出しアクセス権を持つか否かを判定する判定手段、この判定手段により少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについて暗号化を実行する暗号化手段、判定手段より全てのアクセス主体が読み出しアクセス権を持っていると判定されたデータについては該データをそのまま記録し、少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについては前記暗号化手段で暗号化されたデータを記録する第２の記憶媒体により構成されている。

【００１１】また、第２の記憶媒体は記録されるデータとともに該データにあらかじめ付与されたアクセス権情報を記録し、第２の記憶媒体より読み出されたデータに対し該データに付与されたアクセス権情報に基づいて全てのアクセス主体が前記データに対して読み出しアクセス権を持つか否かを判定手段で判定し、該判定手段により少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについて復号化手段により復号化を実行し、判定手段より全てのアクセス主体が読み出しアクセス権を持っていると判定されたデータについては該データをそのまま、あるいは前記少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについては前記復号化手段で復号化されたデータをそれぞれ第１の記憶媒体に書込むように構成されている。

【００１２】

【作用】この結果、本発明によれば、少なくとも一つのアクセス主体が読出アクセス権を持っていないデータについては、守秘の必要のあるデータとして暗号化してバックアップし、全てのアクセス主体が読出アクセス権を持つデータについては、守秘の必要のないデータとして暗号化を行わずにそのままバックアップするようになり、バックアップデータについてのセキュリティ保護とプライバシ保護を確保することができる。

【００１３】

【実施例】以下、本発明の一実施例を図面に従い説明する。

【００１４】図１は同実施例のデータバックアップ装置が適用されるオペレーティングシステムの概略構成を示している。図において、１は複数のファイルを格納可能にしたファイルシステムを構成する磁気ディスクで、この磁気ディスク１はディスク制御部２によりファイルの書込み読み出しを制御されるようになっている。

【００１５】ディスク制御部２には、保護判定部３を接続している。この保護判定部３は、後述するテープ制御部６にも接続していて、磁気ディスク１より読出されたファイル内容または後述する磁気テープ５より読出されたファイル内容について、これらファイルにあらかじめ設定されたアクセス権情報に基づいてすべてのアクセス主体が該ファイルに対して読出アクセス権を有するか否かを判定し、読み出しアクセス保護を行うものである。そして、この保護判定部３での判定結果に基づいて磁気ディスク１より読出されたファイル内容または後述する磁気テープ５より読出されたファイル内容を暗号・復号化部４または磁気テープ制御部５、ディスク制御部２に与えるようにしている。暗号・復号化部４は、周知のＤＥＳ方式などを用いてファイルデータの暗号化または復号化するものである。

【００１６】５は複数のバックアップ用ファイルを格納する磁気テープで、この磁気テープ５は、磁気テープ制御部６によりファイルの書込み読み出しを制御されるようになっている。

【００１７】７は制御部で、この制御部７は、ディスク制御部２、保護判定部３、暗号・復号化部４および磁気テープ制御部６の各制御を行うもので、これら各回路に対して制御指令を出力するものである。次に、以上のように構成した実施例の動作を説明する。

【００１８】この場合、本実施例でバックアップを行う対象となるオペレーティングシステムのファイルシステムでは、磁気ディスク１に格納される個々のファイルについて、アクセス権情報としてＵ、Ｇ、Ｐの３つの属性が付与される。そして、このようなオペレーティングシステムは複数の利用者によって利用されるシステムで、利用者の集合として利用者グループを定義することができるようになっている。

【００１９】ここで、各ファイルに付与される属性Ｕはファイルの所有権を持つ利用者の識別子を保持するものである。また、属性Ｇはそのファイルの所属する利用者グループの識別子を保持するものである。さらに、属性Ｐはそのファイルに対していかなる利用者がいかなるアクセス権を持つかを示す６ビットの２進整数値であり、その第０ビットはＵ属性に示す利用者がそのファイルを読み出す権利を持つか否かを、第１ビットはＵ属性に示す利用者がそのファイルに書き込む権利を持つか否かを、第２ビットはＵ属性に示す利用者ではないがＧ属性に示す利用者グループに所属する利用者がそのファイルを読み出す権利を持つか否かを、第３ビットはＵ属性に示す利用者ではないがＧ属性に示す利用者グループに所

属する利用者がそのファイルに書き込む権利を持つか否かを、第４ビットはＵ属性に示す利用者でもなくなおかつＧ属性に示す利用者グループにも所属しない利用者がそのファイルを読み出す権利を持つか否かを、第５ビットはＵ属性に示す利用者でもなく、かつＧ属性に示す利用者グループにも所属しない利用者がそのファイルに書き込む権利を持つか否かを示している（いずれのビットもその値が１のとき権利を持つことを示し、０のとき持たないことを示す。）。

【００２０】そして、このようなオペレーティングシステムにおけるバックアップ記録は、定期的にファイルシステムでの磁気ディスク１の稼動を停止し、その間に磁気ディスク１の中に存在する全てのファイルについて、その内容を磁気テープ６に複写することによって行なわれる。この場合、オペレーティングシステムによりバックアップの記録を行なうコマンドが提供される。この状態から、バックアップのためのデータ記録は、バックアップを指示するコマンドにより図２に示す処理フローに従って実行される。この場合、ディスク制御部２により、磁気ディスク１よりバックアップしようとするファイルを読み出す（ステップＳ２１）。

【００２１】次に、このようにして読み出したファイルを保護判定部３に与え、ファイルの属性値に基づき読出アクセス保護判定を行う（ステップＳ２２）。この場合、ファイルの内容を読み出す権利が全ての利用者にあるか否かは、そのファイルのＰ属性の第０、第２、第４ビットが全て１であるか否かによって判定される。すなわちＰ属性の第０、第２、第４ビットをそれぞれｐ０，ｐ２，ｐ４と表すと、読み出アクセス保護判定結果ｃは

ｃ＝ｐ０＾ｐ２＾ｐ４

により計算される。（＾は論理積を意味する）

【００２２】そして、ここでの判定結果としてｃの値が１の場合は、ファイルの暗号化は不必要と判断され（ステップＳ２３）、ファイルは直接磁気テープ制御部６に与えられ、磁気テープ５に書込まれる（ステップＳ２５）。

【００２３】一方、保護判定部３の判定結果としてｃの値が０の場合には、ファイルの暗号化は必要と判断され（ステップＳ２３）、ファイルは暗号・復号化部４に与えられる（ステップＳ２４）。暗号・復号化部４では、暗号化が必要と判断されたファイルデータについて周知のＤＥＳ方式などを用いて暗号化を行う。そして、この暗号化されたファイルの内容は、磁気テープ制御部６に与えられ磁気テープ５に書込まれるようになる（ステップＳ２５）。この場合、ファイルに付与されたＵ属性、Ｇ属性、Ｐ属性のそれぞれの値もテープに書込まれるようになる。以下、同様にして磁気ディスク１に格納されたすべてのファイルについてバックアップ処理が行われる。

【００２４】従って、このようにすれば少なくとも一つのアクセス主体が読出アクセス権を持っていないデータについては、守秘の必要のあるデータとして暗号化してバックアップし、全てのアクセス主体が読出アクセス権を持つデータについては、守秘の必要のないデータとして暗号化を行わずにそのままバックアップするようにできるので、バックアップによって保存されるデータに対して効率のよい守秘を得られ、バックアップデータに対するセキュリティやプライバシが侵害される危険性を除去して、これらセキュリティ保護とプライバシ保護を安定して確保することができる。

【００２５】次に、このようにして磁気テープ５に記録されたバックアップデータの復元は、バックアップの復元を指示するコマンドにより図３に示す処理フローに従って実行される。

【００２６】この場合、磁気テープ制御部６により、磁気テープ５より復元しようとするファイルを読み出す（ステップＳ３１）。この場合、上述したバックアップ記録の際に磁気テープ５に記録したＵ属性、Ｇ属性、Ｐ属性のそれぞれの値も読み出す。

【００２７】次に、このようにして読み出したファイルを保護判定部３に与え、ファイルの属性値に基づき読出アクセス保護判定を行う（ステップＳ３２）。この場合、磁気テープ５から復元されたＰ属性の値に基づいて、上述した記録の際に行なった読出アクセス保護判定と同様にして行なわれる。すなわち、磁気テープ５から復元されたＰ属性の第０、第２、第４ビットをそれぞれｐ０′，ｐ２′，ｐ４′と表すと、読出アクセス保護判定結果ｃは

ｃ＝ｐ０′＾ｐ２′＾ｐ４′

により計算される。（＾は論理積を意味する）

【００２８】そして、ここでの判定結果としてｃの値が１の場合は、ファイルの復号化は不必要と判断され（ステップＳ３３）、ファイルは直接ディスク制御部２に与えられ、磁気ディスク１に書込まれる（ステップＳ３５）。

【００２９】一方、保護判定部３の判定結果としてｃの値が０の場合には、ファイルの復号化は必要と判断され（ステップＳ３３）、ファイルは暗号・復号化部４に与えられる（ステップＳ３４）。暗号・復号化部４では、復号化が必要と判断されたファイルデータについて復号化を行う。そして、この復号化されたファイルの内容は、磁気ディスク制御部２に与えられ磁気ディスク１に書込まれるようになる（ステップＳ３５）。以下、同様にして磁気テープ５にバックアップのため格納されたすべてのファイルが磁気ディスク１に復元されることになる。

【００３０】従って、このようにしてもバックアップされたデータについて、少なくとも一つのアクセス主体が読出アクセス権を持っていないデータについては、守秘の必要のあるデータとして復号化して復元し、全てのア

クセス主体が読出アクセス権を持つデータについては、守秘の必要のないデータとして復号化することなく復元できるようになるので、バックアップによって保存されるデータの復元の際もデータに対して効率のよい守秘を得られ、復元されるデータに対するセキュリティやプライバシが侵害される危険性を除去して、これらセキュリティ保護とプライバシ保護を安定して確保することができる。本発明は、他の実施例として、電子メイルシステムにおける通信内容のバックアップに適用することも可能である。

【００３１】この場合、電子メイルシステムにおけるメイルには葉書形式と封書形式の２種類の形式があり、このうちの葉書形式のメイルは比較的安価で提供され、内容はある定まった大きさ以内に制限され、内容の守秘は保証されていないが、封書形式のメイルは比較的高価で提供され、内容の大きさは制限されず、内容の守秘が保証されている。

【００３２】そこで、葉書型式のメイルについては、そのメイルの送信者による読出アクセスと書込アクセスおよび全利用者による読出アクセスを許可し、また、封書型式のメイルについては、そのメイルの送信者による読出アクセスと書込アクセスおよびメイルの受信者による読出アクセスのみを許可する。すなわち、メイルの型式が葉書または封書のいずれかであるかということをアクセス権情報とするようにしている。

【００３３】このメイルシステムにおけるバックアップは、２台のフロッピーディスク装置Ｆ０、Ｆ１を用い、利用者によりメイルの送信要求があったときに葉書型式のメイルはＦ０に、また封書型式のメイルはＦ１にメイルの内容を記録することにより実現している。

【００３４】この場合、図４のフローチャートに示すように、まず、読出アクセス保護判定を行う（ステップＳ４１）。ここで、メイルの内容が全ての利用者に読出可能であるか否かということは、そのメイルが葉書型式であるか否かということと等価であるので、読出アクセス保護判定としては、バックアップ対象となっているメイルの型式が何であるかということを調べる。

【００３５】そして、ここでの判定結果として葉書形式のメイルと判定すると（ステップＳ４２）、内容の暗号化を行なわずにＦ０に記録する（ステップＳ４３）。一方、ステップＳ４２で封書形式のメイルと判定すると、メイルの内容を暗号化して（ステップＳ４４）、Ｆ１に記録するようになる（ステップＳ４５）。

【００３６】従って、電子メイルシステムにおいても、上述したようにバックアップを行う場合と同様にして、バックアップによって保存されるメイルに対して効率のよい守秘を得られ、バックアップメイルに対するセキュリティやプライバシが侵害される危険性を除去して、これらセキュリティ保護とプライバシ保護を安定して確保することができる。なお、本発明は、上記実施例にのみ限定されず、要旨を変更しない範囲で適宜変形して実施できる。

【００３７】

【発明の効果】本発明によれば、データのバックアップにおいて守秘の必要なデータについて、バックアップを通じてのデータのセキュリティやプライバシの侵害の危険性を排除して、セキュリティ保護とプライバシ保護を安定して確保することができる。また、守秘の必要なデータについて暗号化、復号化を行うのみでバックアップを行うようにしているので、不必要な暗号化・復号化の計算を必要とすることなく、効率よくデータのバックアップを実現できる。

【図面の簡単な説明】

【図１】本発明の一実施例の概略構成を示す図。

【図２】図１の実施例の動作を説明するためのフローチャート。

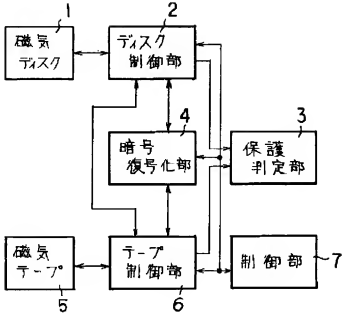
【図３】図１の実施例の動作を説明するためのフローチャート。

【図４】本発明の他の実施例を説明するためのフローチャート。

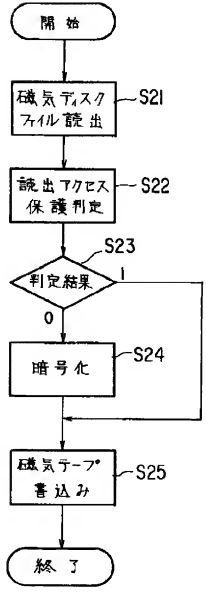
【符号の説明】

１…磁気ディスク、２…ディスク制御部、３…保護判定部、４…暗号・復号化部、５…磁気テープ、６…テープ制御部、７…制御部。

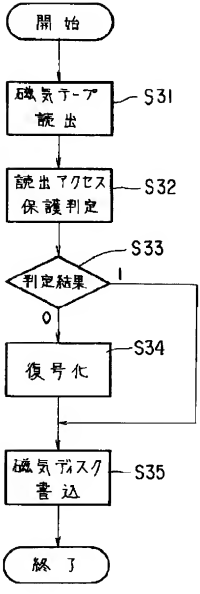
【図1】


1
磁気
ディスク
2
ディスク
制御部
4
暗号
復号化部
3
保護
判定部
磁気
テープ
5
テープ
制御部
6
制御部
7

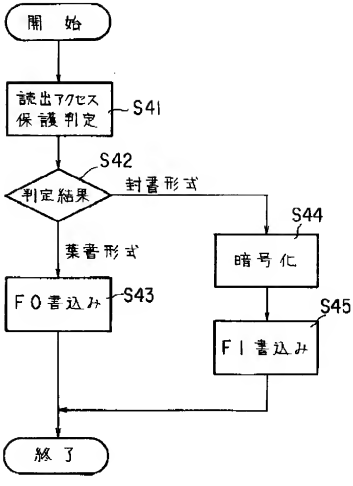
【図2】


開始
磁気ディスク
ファイル読出
S21
読出アクセス
保護判定
S22
S23
判定結果
1
0
暗号化
S24
磁気テープ
書込み
S25
終了

【図3】


開始
磁気テープ読出
S31
読出アクセス保護判定
S32
判定結果
S33
1
0
復号化
S34
磁気ディスク書込
S35
終了

【図4】


開始
読出アクセス保護判定
S41
判定結果
S42
封書形式
葉書形式
暗号化
S44
FO書込み
S43
FI書込み
S45
終了